PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-196085
(43)Date of publication of application : 21.07.1999

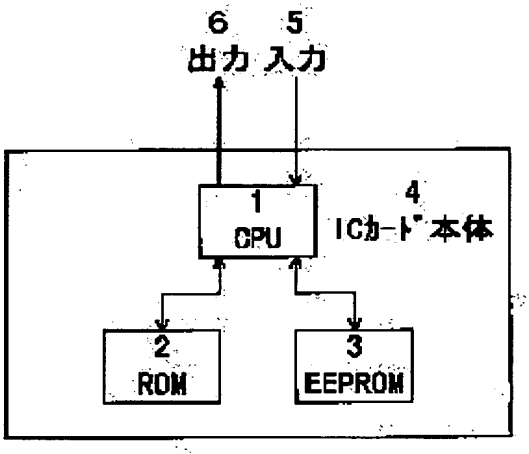
(51)Int.CI. H04L 9/26
G09C 1/00
H04L 9/32

(21)Application number : 09-370202
(22)Date of filing : 25.12.1997

(71)Applicant : MICRO TECHNOLOGY KK
(72)Inventor : SHONO KATSUFUSA

(54) ENCIPHERMENT RESTORING IC CARD

(57)Abstract:
PROBLEM TO BE SOLVED: To attain the safe management of information in an information communication network by turning a chaos encipherment restoring system into hardware by means of a general-purpose IC card that contains a CPU, a ROM and an EEPROM.
SOLUTION: A CPU 1 is mounted on an IC card main body 4, and an instruction set needed for the exclusive processing is printed to a ROM 2. A database for chaos time series and a cipher key are written into an EEPROM 3. A CPU that has the general-purpose numerical and logical arithmetic capability is also available. The data to be enciphered are stored in a memory of a personal terminal in the form of a file. The blocks divided from a digital file to be enciphered are sent to a register of the CPU 1 from an input part 5. Based on an a command, the CPU 1 retrieves a data base 3 and detects a cipher code to transfer it from an output part 6. Restoration is attained by reversing the enciphering process, even if the base 3 is used in common, however since no time element is needed, thereby, another IC card is available for restoration.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－196085

(43)公開日　平成11年(1999)７月21日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｌ	9/26		Ｈ０４Ｌ	9/00	６５９
Ｇ０９Ｃ	1/00	６３０	Ｃ０９Ｃ	1/00	６３０Ａ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｅ

審査請求　未請求　請求項の数１　書面　（全　４　頁）

(21)出願番号　特願平9－370202

(22)出願日　平成９年(1997)12月25日

(71)出願人　591235810
マイクロテクノロジ株式会社
東京都文京区大塚６丁目７番４－302号

(72)発明者　庄野　克房
神奈川県横浜市旭区白根５丁目45番12号

(54)【発明の名称】　暗号化復元用ＩＣカード

(57)【要約】

【目的】　コンピュータと通信を主要な構成要素とする情報通信ネットワークにおいて、個人の情報の安全管理を容易にするディジタルデータ暗号化復元装置を提供する。

【構成】　中央演算装置（ＣＰＵ）を搭載したＩＣカードにおいて、カオス暗号専用の処理行う命令セットをＲＯＭに書き込み、データ量を縮小と検索の高速化をはかるために時間要素を残してテーブル化したカオスのタイムシリーズと暗号鍵をＥＥＰＲＯＭに書き込んでおく。

【特許請求の範囲】
【請求項１】　中央演算装置（ｃｅｎｔｒａｌ　ｐｒｏｃｅｓｓｉｎｇ　ｕｎｉｔ：ＣＰＵと略す）が検索機能をもち、記憶装置（メモリ）に命令セットとカオスのタイムシリーズのデータベースを持つことを特長とする暗号化復元用ＩＣカード。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】コンピュータと通信を主要な構成要素とする今日の情報通信ネットワークにおいては、いろいろなレベルで情報の安全管理が必要とされる。安全管理の手段として暗号が用いられる。
【０００２】ネットワークの中のサーバーに暗号化復元機能をもたせるのは、集団的安全管理の手法である。
【０００３】個人端末において、ユーザ各人が自己責任において情報の安全管理を行う場合もある。本案は個人の情報管理のための暗号化復元用ＩＣカードに関する。
【０００４】
【従来の技術】カオスの観測可能なタイムシリーズを非線形に量子化し、縮退した量子に分割したディジタルブロックを対応させて暗号鍵とし、タイムシリーズ上を検索して暗号化復元を行う、カオスの秩序を利用した暗号化復元の手法は既に知られている。
【０００５】カオスの発生は電子回路的に行っても、非線形写像関数を精度が保証された計算手法によって求めたものでも、いづれでもよい。
【０００６】非線形量子化を非線形ＡＤＣ（アナログディジタル変換器）を用いて回路的に行っても、いったんタイムシリーズを計算機内のメモリに記憶したあと非線形区分を与えて量子化してもよい。
【０００７】カオス暗号の特長は、同じ暗号化すべきディジタルファイルを繰り返し暗号化したとき、同じ暗号鍵を用いても、常に異なる暗号コードが生成されることである。
【０００８】
【発明が解決しようとする課題】カオス暗号は専らソフトウエアとして提供されてきた。情報の安全管理がソフトウエアの管理に置き換えられている。ソフトウエアは誰にでも容易にコピーがとれる。ダウンロードした使用状態からでもコピーがとられる危険がある。これらの危険を回避するために、ＩＣカードのハードウエアとして暗号化復元システムを提供するのが本案である。
【０００９】
【課題を解決するための手段】ＩＣカードには、規模が小さくてもＣＰＵが搭載されているものがある。専用の処理をするための命令セットはＲＯＭに焼き付けられている。カオスタイムシリーズのデータベースと暗号鍵がＥＥＰＲＯＭに書き込まれる。
【００１０】非線形量子化により生成される縮退した量子の量子サイズをそろえたタイムシリーズをそのままＥＥＰＲＯＭに書き込むと、当然のことながら、膨大なデータ量となる。
【００１１】暗号化にあたって検索を行うときには、たとえば８ビット２５６量子に量子化したタイムシリーズでは、検索して発見したデータｙ（ｔ）に対し標準的には４ステップ過去の値ｙ（ｔ－４）を暗号コードとする。時間要素を残してテーブル化することにより検索を高速に実行でき、タイムシリーズのデータを圧縮することができる。また、検索に工夫をすることにより、時間要素を取り除いたテーブルを検索するようにしてもよい。例えば８ビットに量子化した場合、１６行１６列のテーブルとなる。行の並べ方が暗号鍵となる。
【００１２】カオスのタイムシリーズにはフラクタル性が保存されている。タイムシリーズのある範囲のみのデータを検索用のデータベースとしてＥＥＰＲＯＭに書き込んでおくことで、繰り返し暗号化したときに異なる暗号コードが生成されるというカオス暗号の特長が失われることはない。
【００１３】
【作用】ＩＣカードの構成の１例を図１に示す。１は検索機能をもつＣＰＵである。汎用の数値演算及び論理演算能力をもつＣＰＵでよい。必要な命令コードのセットはＲＯＭ２に格納されている。ＥＥＰＲＯＭ３に非線形量子化したカオスのタイムシリーズがデータベースのテーブルとして記憶される。同時に暗号鍵もセットされている。
【００１４】暗号化すべきデータはファイルとして個人用端末のメモリ内に保管されている。暗号化すべきディジタルファイルの分割されたブロックが、入力５からＣＰＵのレジスタに送られ、命令に従ってＣＰＵＩはデータベース３を検索し暗号コードを発見し、出力６から転送する。これが暗号化の過程である。
【００１５】復元は暗号化の逆過程である。データベース３を共通にしても実行できるが、暗号化のデータベース３には時間要素を残したテーブルを用い、暗号コードにカオスの予測不可能な特長を残すようにし、復元用のデータベース３には時間要素は必要としない。暗号化用と復元用に別々のＩＣカード４を用いてもよい。
【００１６】
【実施例】図１の実施例にもとづいて、詳しい具体例を示す。暗号化すべきディジタルファイルを４ビットブロックに分割する場合を説明する。４ビットブロックコードの1つ、例えば、（０１００）がＣＰＵに転送されるものとする。
【００１７】データベース３には１６種類の縮退した量子をもつ８ビットのタイムシリーズが時間要素を残してインストールされている。暗号鍵の配列にしたがって入力コード（０１００）に相当するテーブルの行列が検索され、命令２の指示に従って８ビット暗号コードが１つ選択される。そのコードが（１０１００１０１）という

８ビットコードであったとすると、入力コード（０１００）が８ビット（１０１００１０１）という暗号コードに変換されたことになる。出力６から暗号コード（１０１００１０１）が転送される。この過程を繰り返して、暗号化すべきディジタルファイルのすべての情報が暗号ファイルに変換され、転送される。

【００１８】４ビット入力コード１６種類を１６種類の縮退した量子に対応させる、その組み合わせが暗号鍵である。暗号鍵の発行できる種類は、この場合、１６！＝２．０９×10^{13}通りもある。鍵の発行は距離計算をして、十分離れた距離にある鍵をコンピュータが自動発行・管理する。

【００１９】同じＩＣカードで復元も行う場合には、暗号コード８ビットを入力５から転送してくることによる。上位４ビットと下位４ビットに分割して送ればよい。暗号コードをタイムシリーズのデータベース上で検索し、対応する縮退した量子の４ビットコードを求め、出力６より転送する。

【００２０】この実施例のように４ビットコードが８ビットコードに暗号化され、８ビット暗号コードが４ビットコードに復元されるときには、ＣＰＵは８ビットデータバスをもつ、例えば、Ｚ－８０のような演算装置でよい。

【００２１】暗号化すべきディジタルファイルが文書やデータなどの場合、分割されるディジタルブロックの長さは４ビットか８ビットが適当である。一方、音声のように、周波数分解された音声信号がＡＤ変換され音質を保証するのに上位５ビットを暗号化、転送、復元する場合には、５ビットブロックが適当である。音声の実時間での暗号化復元を実行する場合には、単位ブロックを５ビットにしたシステムの設計をする方が合理的である。

【００２２】暗号鍵の発行にあたって基本操作（シフト、回転、反転、置換など）を加えて、ＩＣカードを階層的に構造化することもできる。

【００２３】カオスの秩序を利用して、階層的に構造化した暗号化復元システムの特長は、Ａという鍵で暗号化したあと、誤ってＢという鍵で復号したとき、当然復号に失敗するが、誤って復号化したファイルから復帰する手法がある。誤ったファイルをいったんＢで暗号化する。そのあとＡで復号すれば、原文にたどり着くことができる。秩序も構造化されているからである。

【００２４】

【発明の効果】暗号化復元処理をソフトウエアで実行するのも便利な手法ではあるが、誰にでも容易にコピーがとれるという点では安全性は損なわれる。ハードウエアの管理はソフトウエアに比べると容易である。本案は、ＣＰＵ、ＲＯＭ及びＥＥＰＲＯＭを搭載した汎用性のあるＩＣカードを用いてカオス暗号化復元システムをハードウエア化した。

【００２５】ＣＰＵ、ＲＯＭ、ＥＥＰＲＯＭを搭載したＩＣカードは、ＣＰＵを共通にしてＲＯＭの命令コードセットやＥＥＰＲＯＭのカオスのデータベースに固有のものを書き込むことにより専用化できる。共通のハードウエア資源を活用して、個別の専用化に対応できる手法である。

【００２６】暗号化用ＩＣカードと復元用ＩＣカードを共通の１枚のカードに統合することもできる。２つに分ける方が処理速度は向上し、音声や画像の実時間処理に都合がよい。

【００２７】ＩＣカードに固有の鍵が与えられるのが本案の原則であるが、鍵の構成に基本操作を加えることにより、複数のＩＣカードに関し暗号化復元システムを階層的に構成することもできる。以上詳しく説明してきたように、本案は情報通信ネットワークにおいて安全な情報管理を実現する新規の手法を提案している。

【図面の簡単な説明】

【図１】暗号化復元用ＩＣカードの構成図である。

【符号の説明】

１　ＣＰＵ
２　ＲＯＭ
３　ＥＥＰＲＯＭ
４　ＩＣカード本体
５　入力
６　出力

【図１】